**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

| | | | |
|---|---|---|---|
| In re the Application of: Janne Suuronen et al. | | Atty. Docket No.: | 004770.00521 |
| Serial No.: | 10/059,182 | Group Art Unit: | 2135 |
| Filed: | January 31, 2002 | Examiner: | Yin Chen Shaw |
| For: | System and Method of Providing Virus Protection At A Gateway | Confirmation No.: | 5357 |

**Appeal Brief**

MAIL STOP APPEAL
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This Appeal Brief is filed in support of Appellants' May 10, 2006, Notice of Appeal. Appeal is taken from the Final Office Action mailed January 25, 2006 (hereinafter, the Office Action). This Appeal Brief is being filed after the mailing of the Pre-Appeal Brief Conference Report of July 5, 2006. Please charge any necessary fees in connection with this Appeal Brief to our Deposit Account No. 19-0733.

## REAL PARTY IN INTEREST
37 C.F.R. § 41.37(c)(1)(i)

The owner of this application, and the real party in interest, is NOKIA Corporation

## RELATED APPEALS AND INTERFERENCES
37 C.F.R. § 41.37(c)(1)(ii)

There are no related appeals and interferences.

## STATUS OF CLAIMS
37 C.F.R. § 41.37(c)(1)(iii)

Claims 1, 3-51, and 53-55 stand rejected. Claims 2 and 52 have been cancelled. Claims 1, 49, and 50 are the independent claims.

Appellants hereby appeal the rejection of claims 1, 3-51, and 53-55.

## STATUS OF AMENDMENTS
37 C.F.R. § 41.37(c)(1)(iv)

The Amendment and Response filed November 7, 2005, has been entered. No Amendment was filed in response to the Final Office Action of January 25, 2006.

## SUMMARY OF CLAIMED SUBJECT MATTER
37 C.F.R. § 41.37(c)(1)(v)

In making reference herein to various portions of the specification and drawings in order to explain the claimed invention, Appellants do not intend to limit the claims; all references to the specification and drawings are illustrative unless otherwise explicitly stated.

The claimed invention relates generally to a system (independent claim 1) or method (independent claim 49) or computer-readable medium (independent claim 50) that provides protection from viruses.

These independent claims relate, to various extents, to a firewall (or system that works with a firewall) that classifies data packets into those packets that can possibly contain a virus and those packets that cannot contain a virus. *Figure 1 and Specification at page 8, line 9, through page 9, line 4*. Those packets that are classified as of a type that cannot contain a virus are passed without further scanning. *Specification at page 8, lines 14-17*. Those packets that are

of a type that can contain a virus are scanned to determine whether the packets indeed contain a virus. *Specification at page 9, lines 1-4.* The specification provides an example of packets relating to audio and video data streams as types of packets that cannot contain viruses. *Specification at page 8, lines 17-20.*

## GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL
37 C.F.R. § 41.37(c)(1)(vi)

A. Claims 1, 3, 20-21, 32, 41-45, 47, 49-52, and 55 stand rejected under 35 U.S.C. § 103 over Fink.

B. Claims 4-5, 11-14, 22-23, 27-28, 33, 36-37, 46, 48, and 53 stand rejected under 35 U.S.C. § 103 over Fink in view of Franczek.

C. Claims 6-8, 24-25, 34, and 54 stand rejected under 35 U.S.C. § 103 over Fink in view of Lyle.

D. Claims 9-10, 15-19, 26, 29-31, 35, and 38-39 stand rejected under 35 U.S.C. § 103 over Fink in view of Lyle and Franczek.

E. Claim 40 stands rejected under 35 U.S.C. § 103 over Fink in view of Radatti.

## ARGUMENT
37 C.F.R. § 41.37(c)(1)(vii)

Applicants respectfully submit that the rejections of record are based on clear factual deficiencies in the applied references. Specifically, the references do not teach or suggest what the Examiner asserts them to teach. Accordingly, a *prima facie* case of obviousness under 35 U.S.C. § 103 has not been established.

Applicants address each of the grounds of rejection in turn.

### *A. Claims 1, 3, 20-21, 32, 41-45, 47, 49-52, and 55 are patentable over Fink*

In order establish a *prima facie* case of obviousness under 35 U.S.C. § 103(a), three criteria must exist: 1) there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine the reference teachings; 2) there must be a reasonable expectation of

success; and 3) the prior art reference(s) must teach or suggest all the claim limitations. See MPEP § 706.02 (j) and *In re Vaeck*, 947 F.2d 488 (Fed. Cir. 1991). Here, the prior art fails to teach or suggest all claim recitations.

Claim 1 recites, *inter alia*:

> " a firewall, which receives the data packets, and
>
> virus scanning engine, …
>
> wherein the firewall classifies the received data packets into packets of a first type which cannot contain a virus and second type which can contain a virus and forwards the data packets of the first type to the destination without testing by the virus scanning engine and forwards the data packets of the second type to the virus scanning engine for testing thereof."

The Examiner uses the primary reference Fink to reject claims 1, 49, and 50. Fink relates to a system for reducing computational work performed by firewalls. At its core, Fink relates to handling packets based on their source while the above-quoted section of claim 1 relates to handling packets based on whether or not a given packet can or cannot potentially contain a virus.

Fink filters packets to allow those packets from unknown sources to be scanned by a firewall. Packets from known trusted sources are permitted to enter a protected network without scanning. *See Fink, column 2, lines 21-49*. The sections relied upon by the Examiner relate to anti-spoofing systems controlled by Fink's pre-filtering module 30. The pre-filtering module checks packets to determine if newly received packets are related to a previously received packet. If the previously received packet was passed to the protected network 12, then the subsequently received related packets are passed to the protected network 12 without scanning by the firewall. *See Fink, column 6, lines 24-33, and column 7, lines 33-47*.

1. Fink Fails To Teach Or Suggest The Claimed Feature Of Virus Scanning

Claim 1 recites a virus scanning engine. Nowhere in Fink is any mention of virus scanning. To address this deficiency of Fink, the Examiner on page 5 of the January 25, 2006,

office action (lines 11-15) asserts that it would have been obvious to use virus scanning in Fink because

> "one would have been motivated to provide security by controlling the traffic being passed, thus preventing illegal communication attempts, both within single networks and between connected networks..."

The Examiner relies on column 7, lines 39-47, of Fink to show filtering at a firewall. However, the filtering of Fink relates to filtering packets to prevent the spoofing of packets. The Examiner seems to suggest that virus-infected packets can be eliminated by the prevention of spoofing.

This position lacks factual support. Whether or not a firewall receives a packet from a known source or an unknown source does **not** indicate whether the packet can contain a virus. Viruses are commonly received from both known and unknown sources.

In response to Applicants' arguments of November 7, 2005, that Fink fails to teach or suggest virus scanning, the Examiner now asserts that Fink *includes* virus scanning by taking an overly broad view of virus scanning:

> "Fink discloses a virus (i.e. causing any kinds of violations and/or spoofing)..." (the January 26, 2006, Office Action, page 32, lines 11-13.)

Applicants *strenuously* object to the suggestion that Fink discloses any type of virus scanning. First, there is no factual basis for defining a virus broad enough to include any type of violations (for instance, phishing scams) or spoofing.

Second, there is no factual basis for believing that a spoofed packet always includes a virus. Whether or not a source of a packet has been spoofed is **independent** as to whether the packet can or cannot contain a virus.

Further, the Examiner has contended that the malicious code (the virus) that is blocked is the code that performs the spoofing. This position is a distortion of what Fink teaches. The spoofing code (malicious or not) resides on a remote system that is sending the packets (with a spoofed return address), not in the packets themselves. There is no suggestion in Fink that any of the spoofing code would be contained in the packets. Accordingly, the alleged spoofing "virus"

would never be detected by Fink because the "virus" would never be contained in the spoofed packets.

Accordingly, because there is no teaching or suggestion to scan for viruses at all in Fink, no *prima facie* case of obviousness has been made. Thus, the rejections of claims 1, 49, and 50 must be withdrawn.

2. Fink Fails To Teach Or Suggest The Claimed Feature Of Classifying Packets

The Examiner relies on Fink, column 6, lines 17-32, and column 7, lines 39-42, to suggest the claimed feature of the firewall classifying packets into:

> "packets of a first type which cannot contain a virus and second type which can contain a virus..." (See claim 1.)

However, Fink fails to teach or suggest this recitation. Fink instead filters packets by determining if the packets have come from a trusted network as specified in the following section of Fink:

> "pre-filtering module 30 performs an anti-spoofing method. Since pre-filtering module 30 may optionally be connected to a plurality of networks, packets can come from any one of these networks. The anti-spoofing method determines whether an IP packet, indicated as originating from a certain network, has indeed arrived from that network. As pre-filtering module 30 knows which network is connected to which interface, pre-filtering module 30 can determine whether a packet received from a particular interface is permitted... Thus, if a packet comes from an allowed source node, is to be sent to an allowed destination, and has arrived through the expected interface, the packet can be processed by pre-filtering module 30." (Emphasis added) See column 7, lines 37-40, of Fink.

Fink fails to examine the type of the received packets and instead only examines the source of the packet. Stated differently, Fink differentiates between spoofed and non-spoofed packets. However, "non-spoofed" is not the same as "cannot contain a virus." For example, a

packet containing a virus received from a known (but virus-infected) source would be passed to the protected network 12 by Fink's pre-filtering module 30. Fink only pre-filters based on source/destination IDs and related information. Therefore, Fink assumes that a packet from a known ID must be safe. Fink is thus vulnerable to viruses that have infected computers whose IDs must be recognized as "safe" by Fink's firewall.

In contrast, claim 1 recites:

> "...forwards the data packets of the first type to the destination without testing by the virus scanning engine and forwards the data packets of the second type to the virus scanning engine for testing thereof."

As Fink fails to teach or suggest at least these features of claim 1, no *prima facie* case of obviousness has been made. Claim 1 is allowable over Fink.

Independent claims 49 and 50 are similarly allowable over Fink.

*B. Claims 4-5, 11-14, 22-23, 27-28, 33, 36-37, 46, 48, and 53 are patentable over Fink in view of Franczek.*

The Examiner next applies Franczek (U.S. Patent No. 6,397,335) in combination with Fink (starting on page 13 of the office action). While Franczek teaches virus scanning, it does not teach allowing packets to pass through a firewall where the screening is based on the type of packets as required by the claims. This is the same failing from which Fink also suffers.

Rather, Franczek determines whether the users are subscribed to the virus filtering system. See Franczek at Figure 3 (step 102) and column 5, lines 29-44. There is no teaching or suggestion in Franczek regarding the filtering of packets based on whether or not they can contain a virus. In Franczek, all packets are either scanned or not scanned for viruses, irrespective of the extent to which they actually *can* contain a virus. Accordingly, the combination lacks the recitation that "...forwards the data packets of the first type to the destination without testing by the virus scanning engine and forwards the data packets of the second type to the virus scanning engine for testing thereof."

As there is no teaching regarding the filtering of packets as set forth in claim 1 and 50, no *prima facie* case of obviousness has been made. Claims 4-5, 11-14, 22-23, 27-28, 33, 36-37, 46, 48, and 53 are allowable over the combination of Fink in view of Franczek.

*C. Claims 6-8, 24-25, 34, and 54 are patentable over Fink in view of Lyle.*

Claims 6-8, 24-25, 34, and 54 stand rejected under 35 U.S.C. § 103 over Fink in view of Lyle. Applicants traverse.

As with Fink, Lyle fails to teach or suggest classifying received packets based on the type of packet. Like Fink, Lyle merely determines whether packets are from an authorized sender. As the combination fails to teach or suggest filtering based on packet type, no *prima facie* case of obviousness has been made. Claims 6-8, 24-25, 34, and 54 are allowable over the combination of Fink in view of Lyle.

*D. Claims 9-10, 15-19, 26, 29-31, 35, and 38-39 are patentable over Fink in view of Lyle and Franczek.*

Claims 9-10, 15-19, 26, 29-31, 35, and 38-39 stand rejected under 35 U.S.C. § 103 over Fink in view of Lyle and Franczek. Applicants traverse.

As indicated above, none of Fink, Lyle, and Franczek teaches or suggests filtering based on whether a packet can or cannot contain a virus. Because there is no teaching in the applied references, combination lacks this recitation as well. Accordingly, no *prima facie* case of obviousness has been made. Claims 9-10, 15-19, 26, 29-31, 35, and 38-39 are allowable over the combination.

*E. Claim 40 is patentable over Fink in view of Radatti.*

Claim 40 stands rejected under 35 U.S.C. § 103 over Fink in view of Radatti.

As with Fink, Radatti fails to teach or suggest filtering packets based on whether or not the packets can or cannot contain viruses. In that Fink also fails to teach or suggest this feature of

independent claim 1, no *prima facie* case of obviousness has been made. Dependent claim 40 is allowable over the combination.

For the above reasons, the rejections of pending claims 1, 3-51, and 53-55 in the Final Office Action fail to establish *prima facie* obviousness. A finding that these claims are allowable is respectfully requested.

For all of the foregoing reasons, Appellants respectfully submit that the final rejection of claims 1, 3-51, and 53-55 is improper and should be reversed.

Respectfully submitted,

BANNER & WITCOFF, LTD.

Dated: December 4, 2006

By: /Christopher R. Glembocki/
Christopher R. Glembocki
Registration No. 38,800

1001 G Street, N.W.
Washington, D.C. 20001-4597
Tel: (202) 824-3000
Fax: (202) 824-3001

## CLAIMS APPENDIX
37 C.F.R. § 41.37(c)(1)(viii)

1. In a communication system including at least a first network coupled to a destination to which transmissions of data packets are made from the first network to the destination, a system for providing virus protection comprising:

a gateway coupled between the first network and the destination, which includes

a firewall, which receives the data packets, and

virus scanning engine, coupled to the firewall, which receives the data packets after reception by the firewall, tests the data packets, passes any data packets, which are tested to not contain a virus to the destination and discards any data packets which are tested and contain a virus,

wherein the firewall classifies the received data packets into packets of a first type which cannot contain a virus and second type which can contain a virus and forwards the data packets of the first type to the destination without testing by the virus scanning engine and forwards the data packets of the second type to the virus scanning engine for testing thereof.

3. A system in accordance with claim 1, wherein:

the virus scanning engine tests the data packets of the second type and forwards those data packets which are tested to not contain a virus to the destination.

4. A system in accordance with claim 1, wherein:

the data packets of the first type contain real time data.

5. A system in accordance with claim 3, wherein:

the data packets of the first type contain real time data.

6. A system in accordance with claim 1, wherein:

the virus scanning engine, when a virus is detected, alerts the firewall that a virus has been detected which, in response to the alert, stops reception of a data stream containing the data packets.

7. A system in accordance with claim 1, wherein:

the virus scanning engine, when a virus is detected, alerts the firewall that a virus has been detected which in response to the alert stops reception of a data stream containing the data packets.

8. A system in accordance with claim 3, wherein:

the virus scanning engine, when a virus is detected, alerts the firewall that a virus has been detected which in response to the alert stops reception of a data stream containing the data packets.

9. A system in accordance with claim 4, wherein:

the virus scanning engine, when a virus is detected, alerts the firewall that a virus has been detected which in response to the alert stops reception of a data stream containing the data packets.

10. A system in accordance with claim 5, wherein:

the virus scanning engine, when a virus is detected, alerts the firewall that a virus has been detected which in response to the alert stops reception of a data stream containing the data packets.

11. A system in accordance with claim 1 wherein:

a buffer which stores the data packets of the second type while the virus scanning engine is processing the data packets of the second type to detect a virus.

12. A system in accordance with claim 3, wherein:

a buffer which stores the data packets of the second type while the virus scanning engine is processing the data packets of the second type to detect a virus.

13. A system in accordance with claim 4, wherein:

a buffer which stores the data packets of the second type while the virus scanning engine is processing the data packets of the second type to detect a virus.

14. A system in accordance with claim 5, wherein:

a buffer which stores the data packets of the second type while the virus scanning engine is processing the data packets of the second type to detect a virus.

15. A system in accordance with claim 6, wherein:

a buffer which stores the data packets of the second type while the virus scanning engine is processing the data packets of the second type to detect a virus.

16. A system in accordance with claim 7, wherein:

a buffer which stores the data packets of the second type while the virus scanning engine is processing the data packets of the second type to detect a virus.

17. A system in accordance with claim 8, wherein:

a buffer which stores the data packets of the second type while the virus scanning engine is processing the data packets of the second type to detect a virus.

18. A system in accordance with claim 9, wherein:

a buffer which stores the data packets of the second type while the virus scanning engine is processing the data packets of the second type to detect a virus.

19. A system in accordance with claim 10, wherein:

a buffer which stores the data packets of the second type while the virus scanning engine is processing the data packets of the second type to detect a virus.

20. A system in accordance with claim 1, wherein:

the firewall drops any received data packets which are tested to be illegal according to firewall rules.

21. A system in accordance with claim 3, wherein:

the firewall drops any received data packets which are tested to be illegal according to firewall rules.

22. A system in accordance with claim 4, wherein:

the firewall drops any received data packets which are tested to be illegal according to firewall rules.

23. A system in accordance with claim 5, wherein:

the firewall drops any received data packets which are tested to be illegal according to firewall rules.

24. A system in accordance with claim 6, wherein:

the firewall drops any received data packets which are tested to be illegal according to firewall rules.

25. A system in accordance with claim 7, wherein:

the firewall drops any received data packets which are tested to be illegal according to firewall rules.

26. A system in accordance with claim 9, wherein:

the firewall drops any received data packets which are tested to be illegal according to firewall rules.

27. A system in accordance with claim 12, wherein:

the firewall drops any received data packets which are tested to be illegal according to firewall rules.

28. A system in accordance with claim 14, wherein:

the firewall drops any received data packets which are tested to be illegal according to firewall rules.

29. A system in accordance with claim 15, wherein:

the firewall drops any received data packets which are tested to be illegal according to firewall rules.

30. A system in accordance with claim 16 wherein:

the firewall drops any received data packets which are tested to be illegal according to firewall rules.

31. A system in accordance with claim 18 wherein:

the firewall drops any received data packets which are tested to be illegal according to firewall rules.

32. A system in accordance with claim 1, wherein:

a packet classification database, coupled to the firewall, which provides information to the firewall which defines the first and second types of data packets;

and a virus detection database, coupled to the virus scanning engine, which provides programming controlling the testing of the data packets of the second type by the virus scanning engine.

33. A system in accordance with claim 4 wherein:

a packet classification database, coupled to the firewall, which provides information to the firewall which defines the first and second types of data packets; and

a virus detection database, coupled to the virus scanning engine, which provides programming controlling the testing of the data packets of the second type by the virus scanning engine.

34. A system in accordance with claim 7 wherein:

a packet classification database, coupled to the firewall, which provides information to the firewall which defines the first and second types of data packets; and

a virus detection database, coupled to the virus scanning engine, which provides programming controlling the testing of the data packets of the second type by the virus scanning engine.

35. A system in accordance with claim 9 wherein:

a packet classification database, coupled to the firewall, which provides information to the firewall which defines the first and second types of data packets; and

a virus detection database, coupled to the virus scanning engine, which provides programming controlling the testing of the data packets of the second type by the virus scanning engine.

36. A system in accordance with claim 11 wherein:

a packet classification database, coupled to the firewall, which provides information to the firewall which defines the first and second types of data packets; and

a virus detection database, coupled to the virus scanning engine, which provides programming controlling the testing of the data packets of the second type by the virus scanning engine.

37. A system in accordance with claim 13 wherein:

a packet classification database, coupled to the firewall, which provides information to the firewall which defines the first and second types of data packets; and

a virus detection database, coupled to the virus scanning engine, which provides programming controlling the testing of the data packets of the second type by the virus scanning engine.

38. A system in accordance with claim 16 wherein:

a packet classification database, coupled to the firewall, which provides information to the firewall which defines the first and second types of data packets; and

a virus detection database, coupled to the virus scanning engine, which provides programming controlling the testing of the data packets of the second type by the virus scanning engine.

39. A system in accordance with claim 18 wherein:

a packet classification database, coupled to the firewall, which provides information to the firewall which defines the first and second types of data packets; and

a virus detection database, coupled to the virus scanning engine, which provides programming controlling the testing of the data packets of the second type by the virus scanning engine.

40. A system in accordance with claim 1, wherein:

the virus scanning engine, upon detection of a virus in the data packets, also alerts the destination that a virus has been detected.

41. A system in accordance with claim 1 wherein:

the destination is a local area network.

42. A system in accordance with claim 1 wherein:

the destination is a personal computer.

43. A system in accordance with claim 1, wherein:

the destination is a second network.

44. A system in accordance with claim 1, wherein:

the first network is a wide area network.

45. A system in accordance with claim 44, wherein:

the wide area network is the Internet.

46. A system in accordance with claim 1, wherein:

the first network is the Internet; and

the destination comprises an Internet service provider coupled to the gateway, a modem coupled to the Internet service provider and one of a local area or personal computer coupled to the modem.

47. A system in accordance with claim 1, wherein:

the virus scanning engine decodes the data packets during determination if the data packets contain a virus.

48. A system in accordance with claim 47, wherein:

the virus scanning engine functions as a proxy for a destination processor which receives the data packets.

49. In a communication system including at least a first network coupled to a destination to which transmissions of data packets are made from the first network to the destination, a gateway coupled between the first network and the destination, which includes a

firewall and a virus scanning engine, said firewall receiving the data packets, a method comprising:

receiving the data packets at the firewall;

classifying the data packets into packets of a first type which cannot contain a virus and a second type which can contain a virus;

transmitting the received data packets of the first type to the destination;

transmitting the received data packets of the second type from the firewall to the virus scanning engine;

testing the data packets with the virus scanning engine; and

transmitting from the virus scanning engine any data packets which are tested by the virus scanning engine to not contain any virus to the destination and the discarding any data packets which are tested to contain a virus.

50. A computer program stored on a storage medium for use in a virus scanning engine in a communication system including at least a first network coupled to a destination to which transmissions of data packets are made from the first network to the destination, a gateway coupled between the first network and the destination, which includes a firewall and the virus scanning engine, coupled to the firewall, said firewall receiving the data packets, the virus scanning engine receiving the data packets after reception by the firewall, passes any data packets, which are tested to not contain a virus to the destination and discards any data packets which are tested to contain a virus, said firewall classifying the received data packets into packets of a first type that cannot contain a virus and a second type that can contain a virus and forwards the data packets of the first type to the destination without testing by the virus scanning engine and forwards the data packets of the second type to the virus scanning engine for testing thereof, the computer program when executed causing the virus scanning engine to execute at least one step of:

testing the data packets for the presence of a virus.

51. A computer program in accordance with claim 50, wherein:

the computer program when executed causes the virus scanning engine to test the data packets of the second type and causes the virus scanning engine to forward those data packets which are tested to not contain a virus to the destination.

53. A computer program in accordance with claim 51, wherein:

the data packets of the first type contain real time data.

54. A computer program in accordance with claim 50, wherein:

the computer program when executed causes the virus scanning engine, when a virus is detected, to alert the firewall that a virus has been detected which, in response to the alert, controls the firewall to stop reception of a data stream containing the data packets.

55. A computer program in accordance with claim 50, the firewall being connected to a packet classification database that provides information to the firewall, the information defining first and second types of data packets and the virus scanning engine being coupled to a virus detection database, wherein the computer program controls the firewall to drop any received data packets that are tested to be illegal according to firewall rules, and

the computer program that controls the testing of the data packets of the second type by the virus scanning engine is provided to the virus scanning engine from the virus detection database.

## EVIDENCE APPENDIX

37 C.F.R. § 41.37(c)(1)(ix)

None.

**RELATED PROCEEDINGS APPENDIX**

37 C.F.R. § 41.37(c)(1)(x)

None.